REMARKS

In the present application, claims 1-23 are pending. Claims 1-23 are rejected. Claims 1 and 9-14 are amended. Claims 15-19 are canceled. As a result of this response, claims 1-14 and 20-23 are believed to be in condition for allowance.

Claim Objections

The Examiner objected to claims 8, 9, and 15 asserting that they are "substantial duplicates" of one another. In the Advisory Action of August 17, 2005 (hereinafter, the "Advisory Action") the Examiner further asserted that "with respect to the objection of claims 8, 9, and 15, the claimed limitations are substantial duplicate [sic] of each other or close in content that they cover the same thing despite a slight difference in wording."

Applicants respectfully disagree with the Examiner's assertions. Claim 8 is drawn to "an access network". Claim 9 is amended herein to more clearly define that it is drawn to "A device for an access network" and, further, "wherein said device is one of an access network element and a ciphering controller." Applicants submit that there is a clear difference between "an access network" and "a device for an access . . . wherein said device is one of an access network element and a ciphering controller". It is further submitted that the difference between the two exceeds "a slight difference in wording" as asserted.

Claim 15 is canceled herein without prejudice or disclaimer and, therefore, the Examiner's rejection of claim 15 is rendered moot.

Claim Rejections – 35 USC § 102

The Examiner rejected claims 1-23 as being anticipated by Berenzweig (U.S. Patent 6,584,310). Specifically, the Examiner asserted that Berenzweig "discloses "a communication network [,] an access network element, or ciphering controller, and a method comprising a user equipment, an access network and a plurality of core networks, wherein said user equipment is configured to be simultaneously in communication with at least two of said plurality of core networks, said communication network comprising: Berenzweig discloses at least two networks wherein each has means of communicating separate ciphering

communications to the access network that meets the recitation of means for communicating separate ciphering parameters to said access network from said at least two of said core networks, for example (see column 3, line 45 through column 4, line 7)". The Examiner further asserted that "Berenzweig discloses means for receiving separate ciphering parameters to said access network from said at least two of said core networks, for example (see column 5, lines 20-23 and lines 5, 29-31)." Lastly, the Examiner asserted that "Berenzweig also discloses means for selecting either the triplets or shared secret key for ciphering between the user and the at least two of the core networks that meets the recitation of said access network comprising means for selecting one of said separate ciphering parameters for ciphering the communications between said user equipment and said at least two of said plurality of core networks in said access network, for example (see columns 3, line 45 through column 4, line 7 and see one example illustrated in column 6, lines 35-63)."

Applicants respectfully disagree with Examiner's characterization of the teachings of Berenzweig vis-à-vis the recitations of the claims. Claim 1 is taken as representative of distinctions over Berenzweig and recites:

> 1. A communication network comprising a user equipment, an access network and a plurality of core networks, said communication network comprising:
> means for **communicating separate ciphering parameters** to said access network from said at least two of said core networks; and
> means for **selecting one of said separate ciphering parameters** for ciphering communications between said user equipment and said at least two of said plurality of core networks in said access network,
> wherein said user equipment is configured to be **simultaneously in communication with at least two of said plurality of core networks**. (emphasis added).

As will be shown, Berenzweig does not teach or disclose user equipment "configured to be simultaneously in communication with at least two of said plurality of core networks", "communicating separate ciphering parameters to said access network", or "selecting one of said separate ciphering parameters".

Berenzweig discloses, in general, translation between different authentication schemes when a mobile station is roaming between networks. A first authentication scheme (triplets) is used in a first network and a second authentication scheme (shared secret data, SSD) is used in a second network. There is an authentication interoperability function (AIF) which translates between the first and second authentication schemes. (see abstract) In this manner, a mobile station native to the second network may roam in the first network and authenticate itself towards the first network using the first authentication scheme.

For example, with reference to Fig. 9, Berenzweig shows a mobile station native to the second network 220 using SSD for authentication. The mobile station authenticates itself to the first network 218 using triplets for authentication. The Visitor Location Register requests a triplet from the AIF, which generates triplets from the SSD information received from the Home Location Register of the second network.

In contrast, claim 1 recites an access network over which the user equipment is "simultaneously in communication with at least two of said plurality of core networks". Berenzweig teaches the presence of two networks between which a mobile station roams. Berenzweig does not disclose a mobile station simultaneously in communication with at least two core networks when roaming in either of the two access networks. As a result, Berenzweig fails to teach or otherwise disclose user equipment "configured to be simultaneously in communication with at least two of said plurality of core networks" as claimed. There is no suggestion in Berenzweig that a roaming mobile station has separate, simultaneous communications with two core networks.

More fundamentally, Applicants respectively disagree with the Examiner's assertion that "Berenzweig discloses means for receiving separate ciphering parameters to said access network from said at least two of said core networks, for example (see column 5, lines 20-23 and lines 5, 29-31)." The Examiner's citation refers to Fig. 9. As is clear from the reference, as well as examination of Fig. 9, the VLR receives only one triplet from the AIF (see column 5, lines 20-21). Put simply, Berenzweig teaches that the AIF enables the same mobile station to be authenticated in disparate networks. The AIF is between the networks themselves (col. 3, lines 55-62, Figs. 7-11) and operates so that only one triplet is sent to the mobile sterminal. As such, Berenzweig discloses receiving only one ciphering parameter in the access network.

Therefore, Berenzweig fails to teach "communicating separate ciphering parameters to said access network" as is claimed. Furthermore, as Berenzweig teaches the reception of only one ciphering parameter, there is no teaching of "selecting one of said separate ciphering parameters" as recited in claim 1.

Lastly, the Examiner references column 6, lines 35-63, which references Fig. 10, to support the assertion that "Berenzweig also discloses means for selecting either the triplets or shared secret key for ciphering between the user and the at least two of the core networks that meets the recitation of said access network comprising means for selecting one of said separate ciphering parameters for ciphering the communications between said user equipment and said at least two of said plurality of core networks in said access network". In fact, Berenzweig discloses that the AIF receives two triplets from the HLR of the first network. However, both triplets are used to calculate the shared secret data SSD to be transmitted to the VLR of the second network. Therefore, the input ciphering parameter of the VLR is from only one network and, thus, teaches directly away from separate ciphering parameters from at least two core networks. Berenzweig thereby fails to once again teach "communicating separate ciphering parameters to said access network from said at least two of said core networks", and "selecting one of said separate ciphering parameters" as claimed.

For the aforementioned reasons, Berenzweig fails to teach or suggest numerous elements recited in claim 1. As a result, Applicants respectfully traverse the Examiner's grounds for rejection. Claim 1 is therefore in condition for allowance. As claims 8 and 9 recite similar limitations, they are likewise deemed to be in condition for allowance for the reasons recited above with reference to claim 1. As all of claims 2-7, 10-14, and 20-23 depend upon claim 1, 8, and 9, they are likewise in condition for allowance.

The Advisory Action

In the Advisory action, the Examiner further asserted that, with respect to claim 1, "Berenzweig discloses in column 3, lines 55-67 means for selecting SSD or triplet to cipher communications between the user and at least two of the core networks (HLR and VLR). In addition, each core network communicates separate cipher parameters as claimed; for example column 6, lines 35-50 stats [sic] two triplets are sent to the AIF from the HLR. For

at least the reasons cited above and in the office action, the request for reconsideration has been considered but does not place the application in condition for allowance."

Applicants respectfully disagree with Examiner's assertion. Specifically, acceptance of the Examiner's characterization of the teachings of Berenzweig leads to the unavoidable conclusion that Berenzweig fails to teach or disclose numerous elements of claim 1. Specifically, as will be shown below, Berenzweig fails to teach communicating separate ciphering parameters to said access network from at least two core networks, selecting one of the separate ciphering parameters in the access network, and ciphering communications between the user equipment and the at least two core networks in the access network as claimed.

Applicants proceed under the assumption, based upon the Examiner assertion that "Berenzweig discloses . . . at least two of the core networks (HLR and VLR)", that the VLR and HLR are considered analogous to the "at least two of said core networks" as recited in claim 1. The teachings of Berenzweig vis-a-vis the recitations of claim 1, are then seen to disclose as follows.

As claim 1 makes it clear that the access network and the plurality of core networks are separate entities, the VLR (visitor location register of core network 1) and HLR (a home location register of core network 2) cannot be located in an access network. This logically follows from the fact, noted above, that the VLR 308 and the HLR 303 are deemed to form the two core networks as recited in claim 1. Therefore, the only element that is located in the access network of Berenzweig is the roaming mobile station (MT 311 and UIM 312). The roaming mobile station is only disclosed to be capable of communication with one of the core networks, i.e. the visited network comprising the VLR. It is true that the some information can be fetched by the visited core network from the HLR of the home core network. However, there is no disclosure or suggestion in Berenzweig that the roaming mobile station in an access network has simultaneous separate communication connections with two core networks. Rather, as is discussed more fully below, the mobile station of Berenzweig in an access network communicates with one core network only.

As disclosed in Figure 9 and the accompanying text at col. 5, line 20 to col. 6, line35, Berenzweig discloses that a mobile station 310 in an access network communicates with a

visited core network (VLR 304). The VLR requests a triplet for the AIF, which in turn requests a SSD from the HLR 306 of the home network of the user. The AIF generates a triplet and returns the triplet to the VLR. The VLR informs the mobile station located in the access network about a security parameter based on the triplet received from the AIF. No separate ciphering parameters are communicated in the access network, and nothing is selected in the access network. Furthermore, in Figure 9, the mobile station in an access network communicates directly with **only one** core network (VLR).

In addition, **only one** security parameter is delivered to the access network via one channel of communications between an element in the access network and one core network. There is, therefore, **no selection of security parameters** in any network element, not to mention a means for selecting a parameter in the access network from parameters communicated from at least two core networks.

As disclosed in Figure 10 and the accompanying text at col. 6, line 36 and following, Berenzweig discloses a mobile station that, again, communicates with only one core network (VLR). The VLR, and not an element of an access network, then requests a SSD from the AIF. The AIF then requests triplets from the HLR, and, in response to receiving two triplets, the AIF generates a SSD using both triplets. The AIF then sends the SSD to the VLR, and the VLR informs the mobile station in the access network about a security parameter based on the SSD received from the AIF.

Thus, in Figure 10, the mobile station in the access network communicates with **only one** core network (VLR). **Only one** security parameter is delivered to the access network. And there is **no selection of security parameters** in any network element; both received triplets are used for generating the SSD, and therefore there cannot be any disclosure or suggestion that any selection would occur in the access network..

Lastly, in the interest of completeness, assuming arguendo that the AIF were located in the VLR (see col. 3, lines 55-67), the VLR would still, in accordance with the Examiner's interpretation, be located in the core network. So even in this AIF-in-VLR case, the mobile station communicates only with one core network, only one security parameter is delivered to the access network and there is no selection of security parameters in any network element, not to mention selection in an element located in an access network as is claimed. As a result

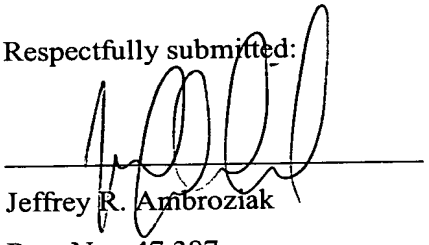
of these deficiencies in the teachings of Berenzweig vis-à-vis the recitations of claim 1, claim 1 is in condition for allowance. As claims 8 and 9 both recite elements in general accord with the those elements of claim 1 discussed above, claims 8 and 9 are in condition for allowance for the reasons stated above.

With reference once again to the Advisory Action, the Examiner asserted that, with reference to claim 1, "applicant argues that the reference does not disclose "simultaneously" in communication; this is only disclosed in the preamble of the claim." Claim 1 has been amended to more clearly recite the above referenced element in a portion of the claim external to the preamble.

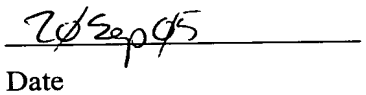
An earnest and thorough attempt has been made by the undersigned to resolve the outstanding issues in this case and place same in condition for allowance. If the Examiner has any questions or feels that a telephone or personal interview would be helpful in resolving any outstanding issues which remain in this application after consideration of this amendment, the Examiner is courteously invited to telephone the undersigned and the same would be gratefully appreciated.

It is submitted that the claims herein patentably define over the art relied on by the Examiner and early allowance of same is courteously solicited.

Respectfully submitted:



Jeffrey R. Ambroziak
Reg. No.: 47,387



Date

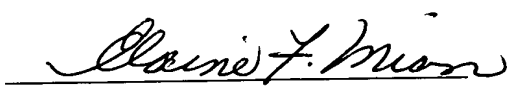
Customer No.: 29683
HARRINGTON & SMITH, LLP
4 Research Drive
Shelton, CT 06484-6212

Telephone: (203)925-9400
Facsimile: (203)944-0245
email: hsmith@hspatent.com

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

9/20/2005
Date



Name of Person Making Deposit